The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A system for determining whether a packed executable is malware, the system comprising:

a malware evaluator for determining whether incoming data is malware; and

an unpacking module that receives a packed executable from the malware evaluator and returns an unpacked executable corresponding to the packed executable;

wherein the malware evaluator, upon receiving incoming data, determines whether the incoming data is a packed executable, and if so, provides the packed executable to the unpacking module and receives from the unpacking module an unpacked executable, and determines whether the unpacked executable is malware.

2. A system for unpacking a packed executable for evaluation as malware, the system comprising:

a set of unpacker modules, the set of unpacker modules comprising at least one unpacker module and wherein each unpacker module corresponds to executable code for unpacking a particular type of packed executable; and

an unpacking manager, wherein the unpacking manager, upon obtaining a packed executable, selects an unpacker module from the set of unpacker modules to unpack the packed executable according to the type of the packed executable, and executes the selected unpacker module which generates an unpacked executable corresponding to the packed executable.

3. The system of Claim 2, wherein each unpacker module in the set of unpacker modules implements a confirmation interface routine for confirming whether the unpacker module is capable of unpacking the packed executable; and

wherein the unpacking manager selects an unpacker module from the set of unpacker modules to unpack the packed executable by:

iteratively calling the confirmation interface routine of each unpacker module in the set of unpacker modules until an unpacker module responds affirmatively to the call of its confirmation interface routine indicating that it can unpack the packed executable; and

selecting that unpacker module that responded affirmatively.

4. A method for determining whether incoming data is malware, the method comprising:

intercepting incoming data directed to a computing device;

determining whether the incoming data is a packed executable; and

if the incoming data is a packed executable:

generating an unpacked executable, the unpacked executable corresponding to the packed executable; and

determining whether the packed executable is malware by evaluating whether the unpacked executable is malware.

5. A method for unpacking a packed executable for evaluation as malware, the method comprising:

obtaining a packed executable;

selecting an unpacker module from a set of unpacker modules operable to unpack the packed executable; and

executing the selected unpacker module, thereby generating an unpacked executable corresponding to the packed executable.

6. An extensible unpacking module for unpacking a packed executable for evaluation as malware, the system comprising:

an set of unpacker modules comprising at least one unpacker module, wherein each unpacker module corresponds to executable code for unpacking a packed executable of a particular type, wherein the set of unpacker modules is dynamically extensible such that unpacker modules may be selectively added or removed to the set of unpacker modules; and

an unpacking manager, wherein the unpacking manager, upon obtaining a packed executable, selects an unpacker module from the set of unpacker modules to unpack the packed executable according to the type of the packed executable, and executes the selected unpacker module which generates an unpacked executable corresponding to the packed executable.